We claim:

1. A method for conducting secure communications, comprising:

(a) connecting a user device via a publicly-accessible network to a server;

(b) receiving a certificate;

(c) calculating an identifier of the received certificate and converting it to a character string;

(d) modifying the string by removing at least one random character from the string;

(e) displaying the modified string;

(f) receiving, from a user previously provided with the identifier through a trusted medium, input corresponding to the at least one removed character; and

(g) continuing connection to the server only if the user input matches the at least one removed character.

2. The method of claim 1, further comprising randomly selecting multiple characters for removal.

3. The method of claim 2, wherein the randomly selected characters are replaced with a character indicating the replacement.

4. The method of claim 2, wherein the modified string is displayed with spaces replacing the removed characters.

5. The method of claim 1, wherein the device is a mobile telephone and the at least one removed character is a digit.

6. The method of claim 1, wherein receiving the certificate comprises receiving the certificate from a certification authority.

7. The method of claim 1, wherein the position of the at least one character removed from the string is different during a subsequent connection attempt.

8. The method of claim 1, wherein the at least one removed character is removed based on the capabilities of the user device.

9. The method of claim 1, wherein receiving input corresponding to the at least one removed character comprises receiving input from a user previously provided with the identifier through a one of the mail or a company newsletter.

10. The method of claim 1, wherein the at least one removed character is a digit, and wherein no non-digit characters are removed.

11. The method of claim 1, further comprising:

repeating steps (a) through (g) on each attempt to connect the device to the server.

12. A device for secure communication with a server via a publicly accessible network, comprising:

an interface to a publicly accessible network; and

a processor configured to perform steps comprising:

receiving, via the interface, a certificate from a remotely located server,

calculating an identifier of the received certificate and converting it to a character string,

modifying the string by removing at least one random character from the string,

displaying the modified string,

receiving, from a user of the device previously provided with the identifier through a trusted medium, input corresponding to the at least one removed character, and

continuing connection to the server only if the user input matches the at least one removed character.

13. A machine-readable medium having machine-executable instructions for performing steps comprising:

(a) connecting a user device via a publicly-accessible network to a server;

(b) receiving a certificate;

(c) calculating an identifier of the received certificate and converting it to a character string;

(d) modifying the string by removing at least one random character from the string;

(e) displaying the modified string;

(f) receiving, from a user previously provided with the identifier through a trusted medium, input corresponding to the at least one removed character; and

(g) continuing connection to the server only if the user input matches the at least one removed character.

14. A method for conducting secure communications, comprising:

(a) connecting a user device via a publicly-accessible network to a server;

(b) receiving a certificate;

(c) receiving a modified identifier, the identifier having previously been calculated for the certificate outside of the user device and modified outside of the user device by removal of at least one random character;

(e) displaying the modified identifier;

(f) receiving, from a user previously provided with the identifier through a trusted medium, input corresponding to the at least one removed character; and

(g) continuing connection to the server only if the user input matches the at least one removed character.